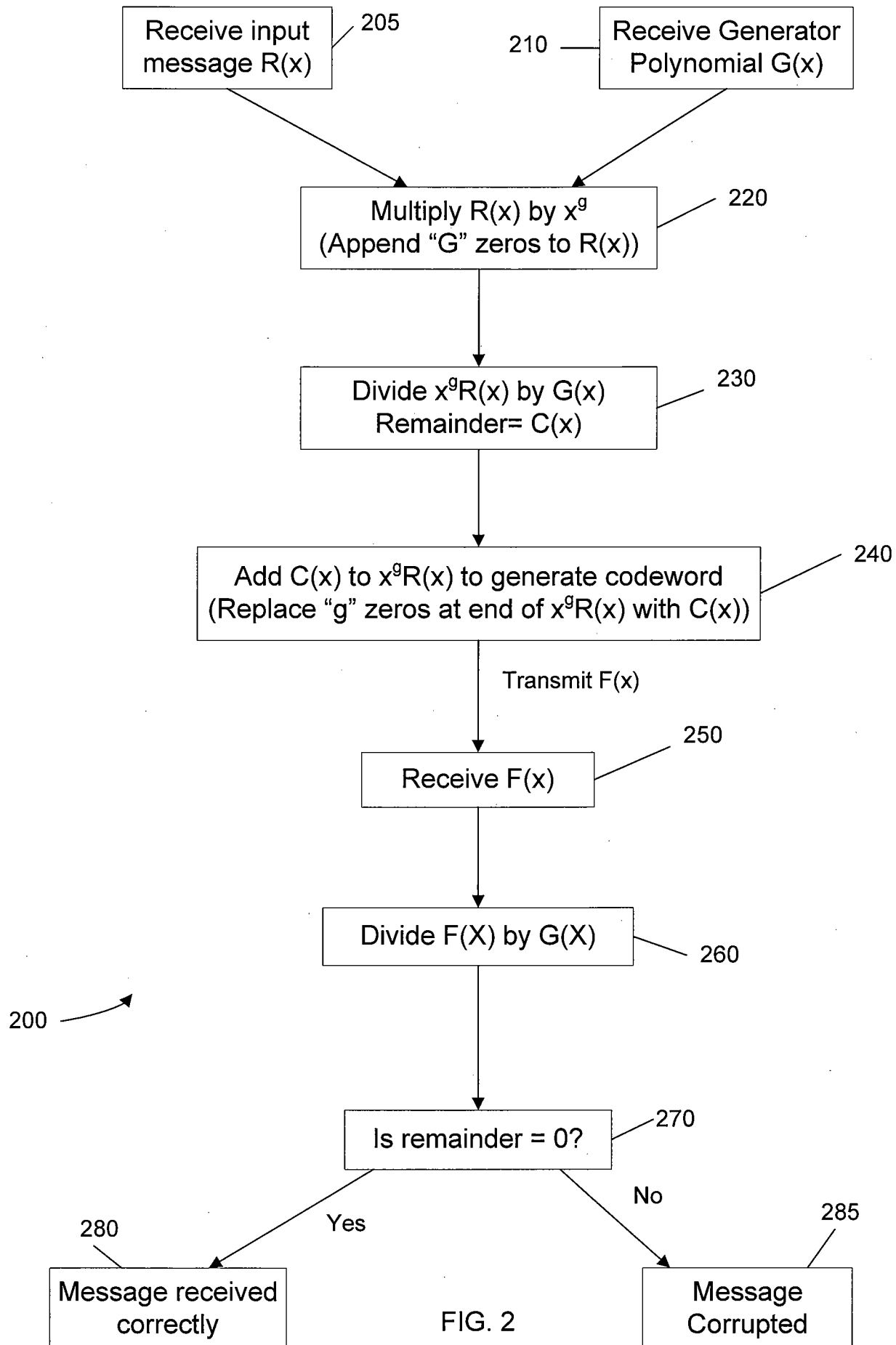


FIG. 1



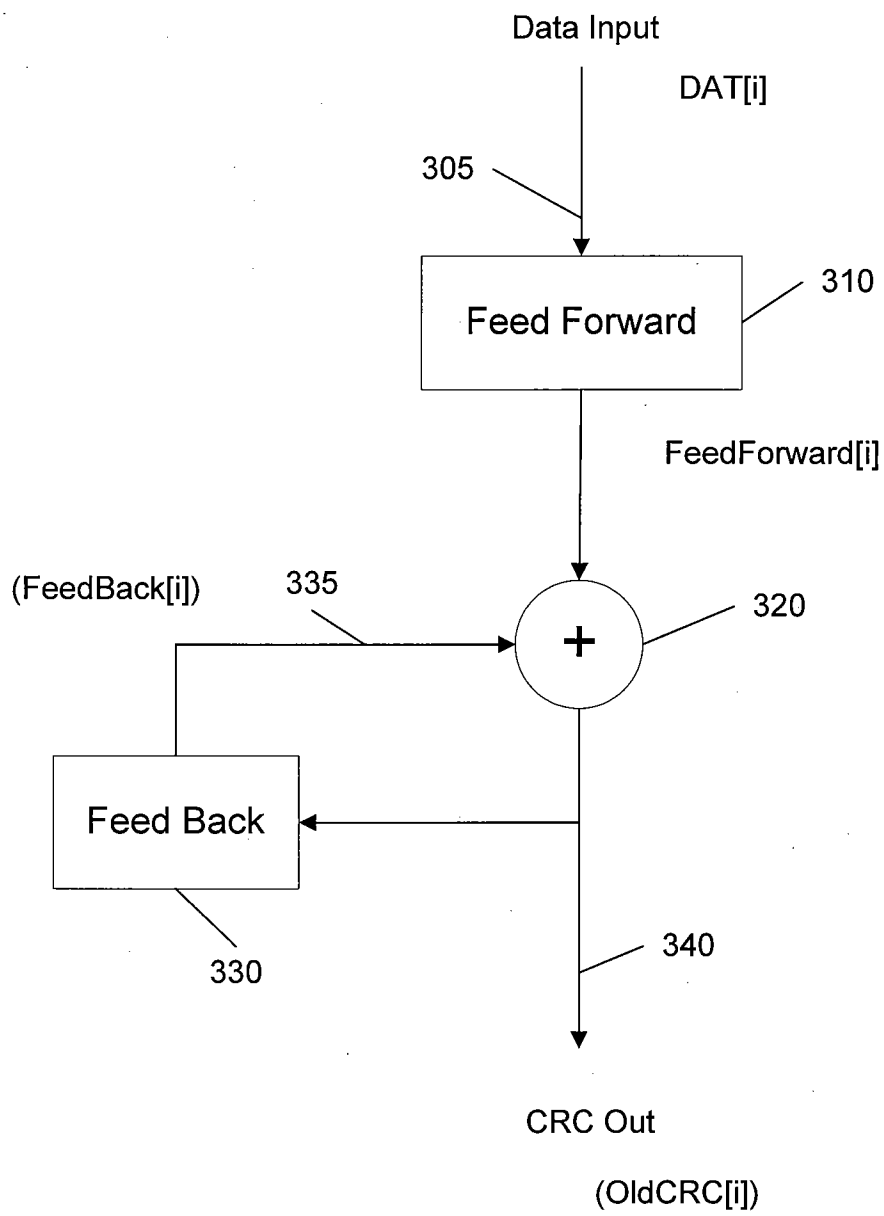
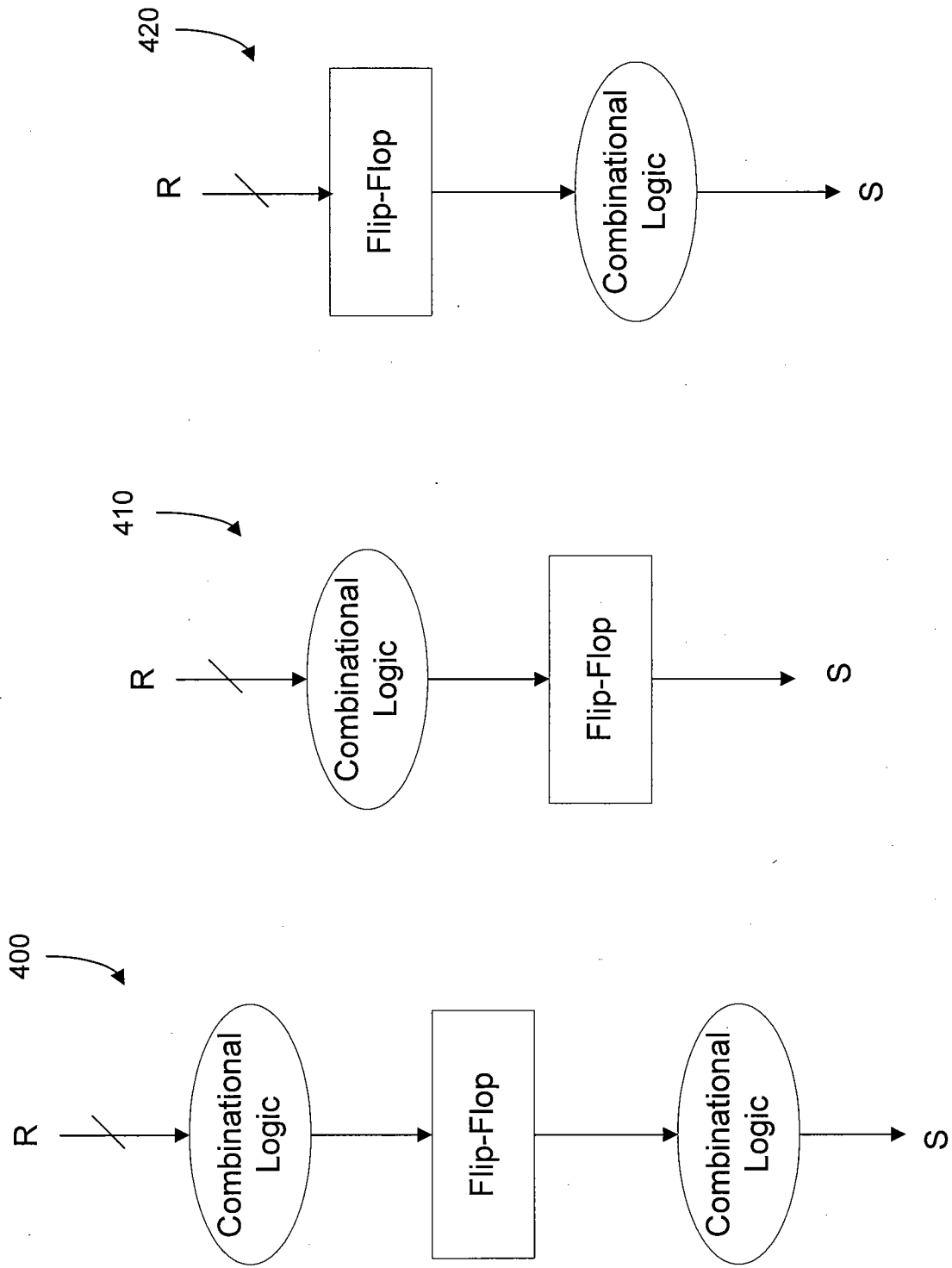


FIG. 3

FIG. 4



$$X^g(W_1 W_2 W_3) \bmod G = X^g(W_1 \cdot X^{2W} + W_2 \cdot X^W + W_3) \bmod G \sim 500$$

$$(W_1 \cdot X^{2W} + Z \cdot X^W + Z) \bmod G \sim 505$$

$$(Z \cdot X^{2W} + W_2 \cdot X^W + Z) \bmod G \sim 510$$

$$\frac{(Z \cdot X^{2W} + Z \cdot X^W + W_3) \bmod G \sim 515}{(W_1 \cdot X^{2W} + W_2 \cdot X^W + W_3) \bmod G \sim 520}$$

$$= (W_1 W_2 W_3) \bmod G \sim 522$$

$$\text{IF: } (W_1) \bmod G = S_1 \sim 530$$

$$(W_2) \bmod G = S_2 \sim 540$$

$$(W_3) \bmod G = S_3 \sim 550$$

$$\text{THEN: } (S_1 \cdot X^{2W} + S_2 \cdot X^W + S_3) \bmod G \sim 560$$

$$= (W_1 \cdot X^{2W} + W_2 \cdot X^W + W_3) \bmod G \sim 565$$

$$\text{So: } (S_1 \cdot X^{2W} + Z \cdot X^W + Z) \bmod G \sim 570$$

$$(Z \cdot X^{2W} + S_2 \cdot X^W + Z) \bmod G \sim 575$$

$$(Z \cdot X^{2W} + Z \cdot X^W + S_3) \bmod G \sim 580$$

$$\frac{(Z \cdot X^{2W} + Z \cdot X^W + S_3) \bmod G \sim 580}{(W_1 \cdot X^{2W} + W_2 \cdot X^W + W_3) \bmod G \sim 590}$$

$$= (W_1 W_2 W_3) \bmod G \sim 595$$

FIG. 5

$$X^g \cdot (W_1 W_2 W_3) \bmod G \quad 600$$

$W_1$   
 $W_2$   
 $W_3$

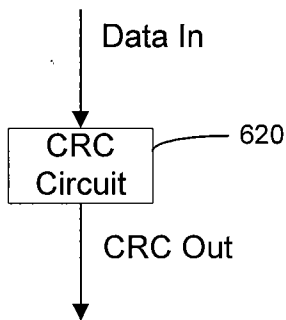
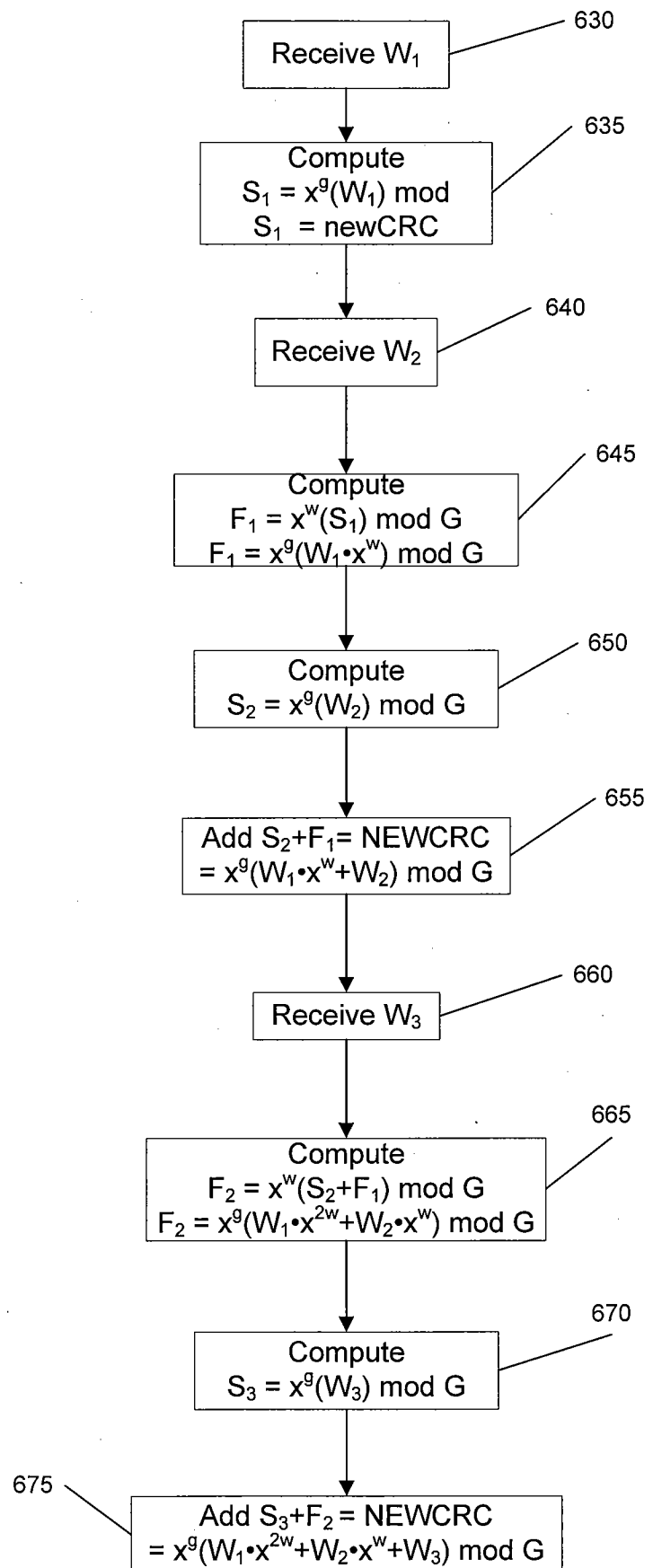


FIG. 6



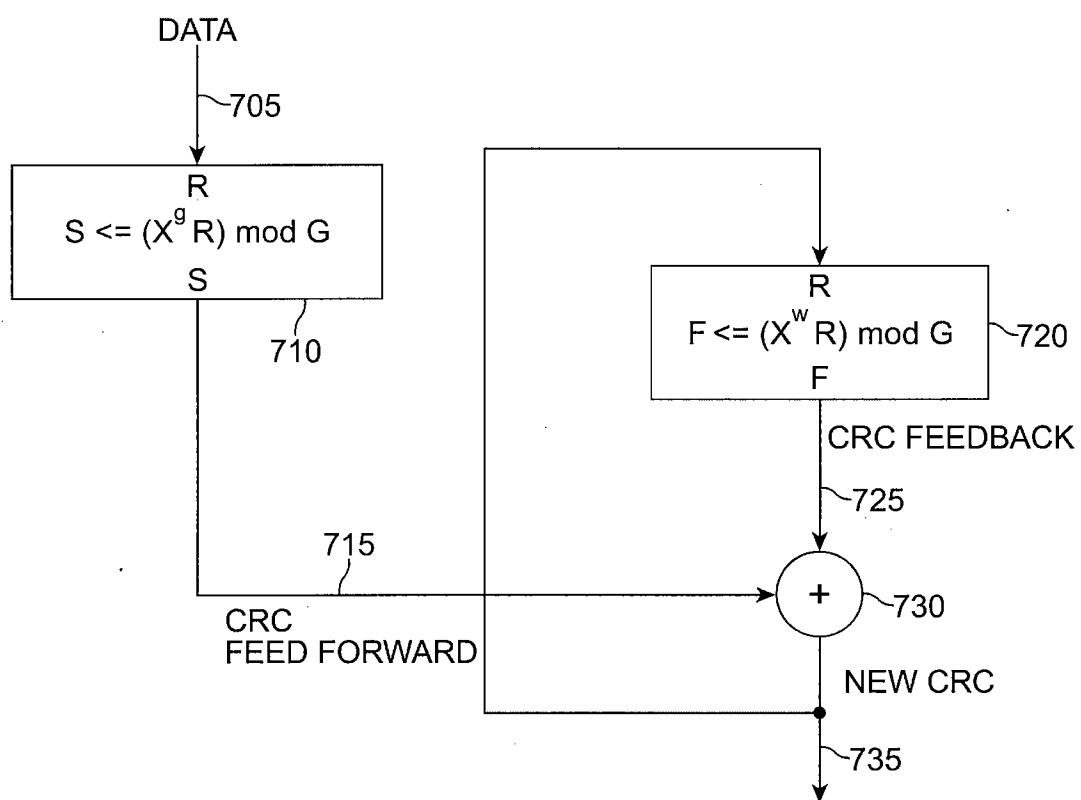


FIG. 7

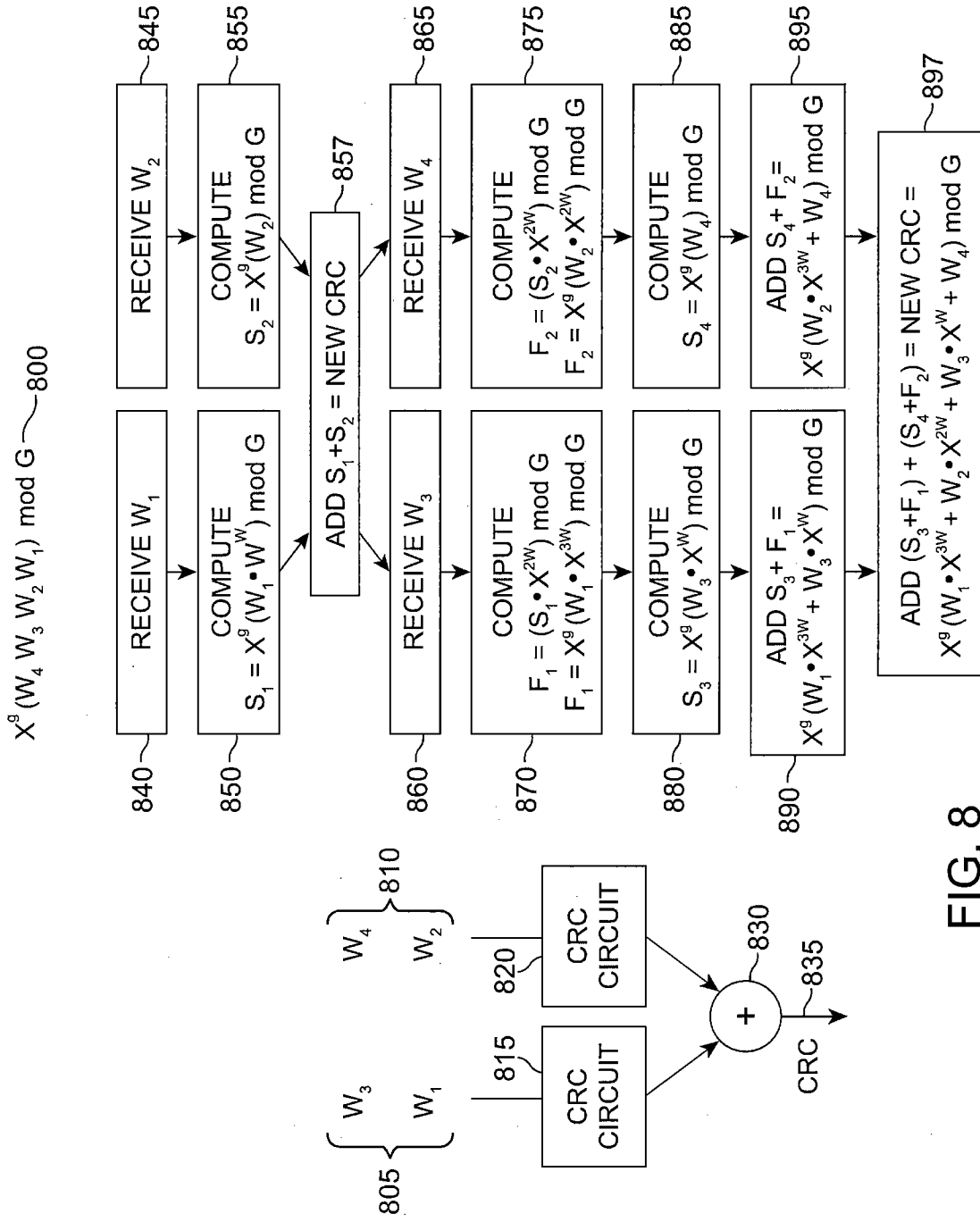


FIG. 8



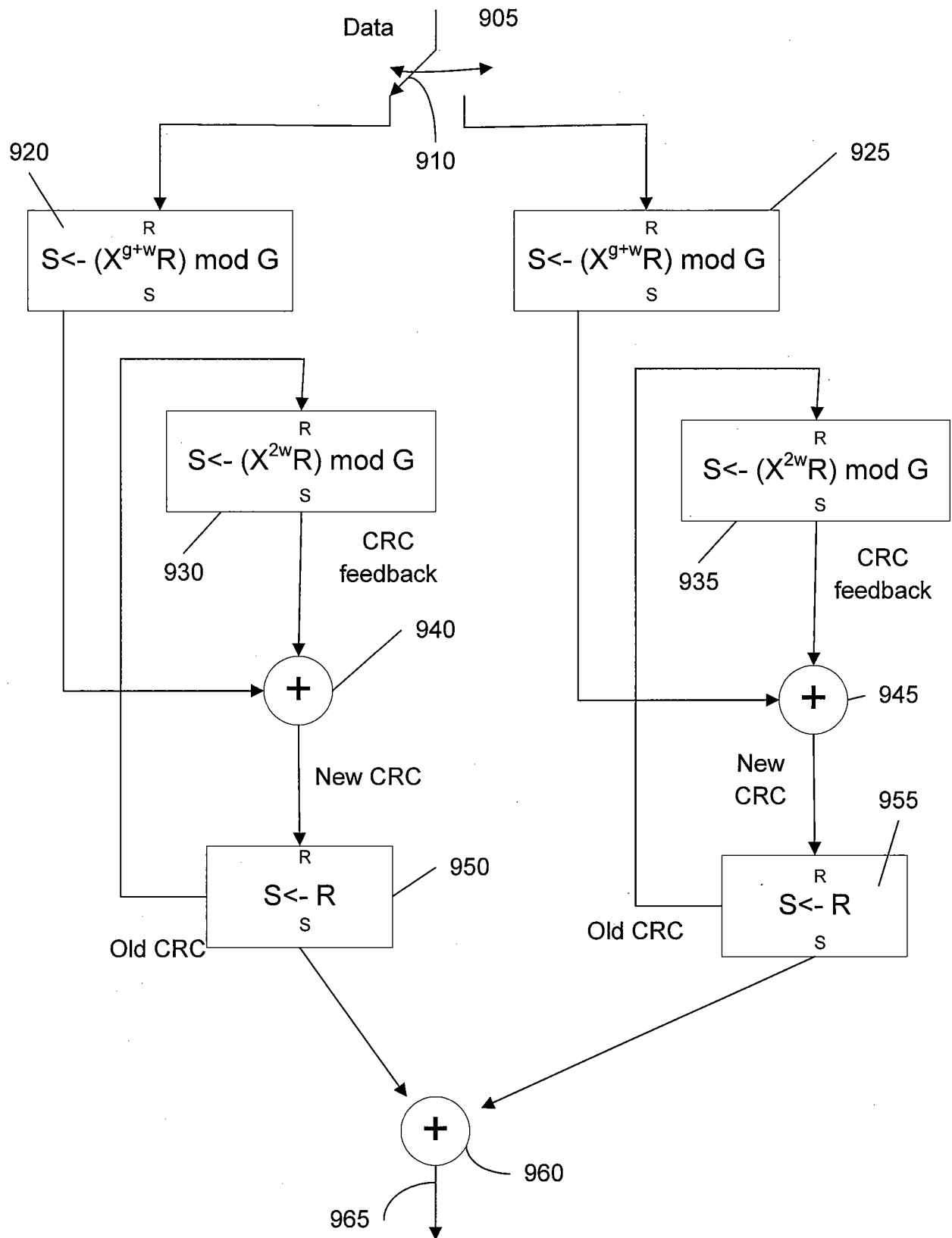


FIG. 9

$$\begin{aligned}
 X^g(W_1 W_2 W_3) \bmod G &= X^g(W_1 \cdot X^{2W} + W_2 \cdot X^W + W_3) \bmod G \\
 (W_1 \cdot X^{2W} + Z \cdot X^W + W_3) \bmod G &\sim_{1015} \quad \quad \quad 1010 \\
 (Z \cdot X^{2W} + W_2 \cdot X^W + Z) \bmod G &\sim_{1020} \\
 \hline
 (W_1 \cdot X^{2W} + W_2 \cdot X^W + W_3) \bmod G &\sim_{1025}
 \end{aligned}$$

$$\text{IF: } (W_1) \bmod G = S_1 \sim_{1030}$$

$$(W_2) \bmod G = S_2 \sim_{1035}$$

$$(W_3) \bmod G = S_3 \sim_{1040}$$

$$\text{THEN: } (S_1 \cdot X^{2W} + Z \cdot X^W + S_2) \bmod G \sim_{1045}$$

$$(Z \cdot X^{2W} + S_2 \cdot X^W + Z) \bmod G \sim_{1050}$$

$$(W_1 \cdot X^{2W} + W_2 \cdot X^W + W_3) \bmod G \sim_{1055}$$

$$= (W_1 W_2 W_3) \bmod G \sim_{1060}$$

FIG. 10

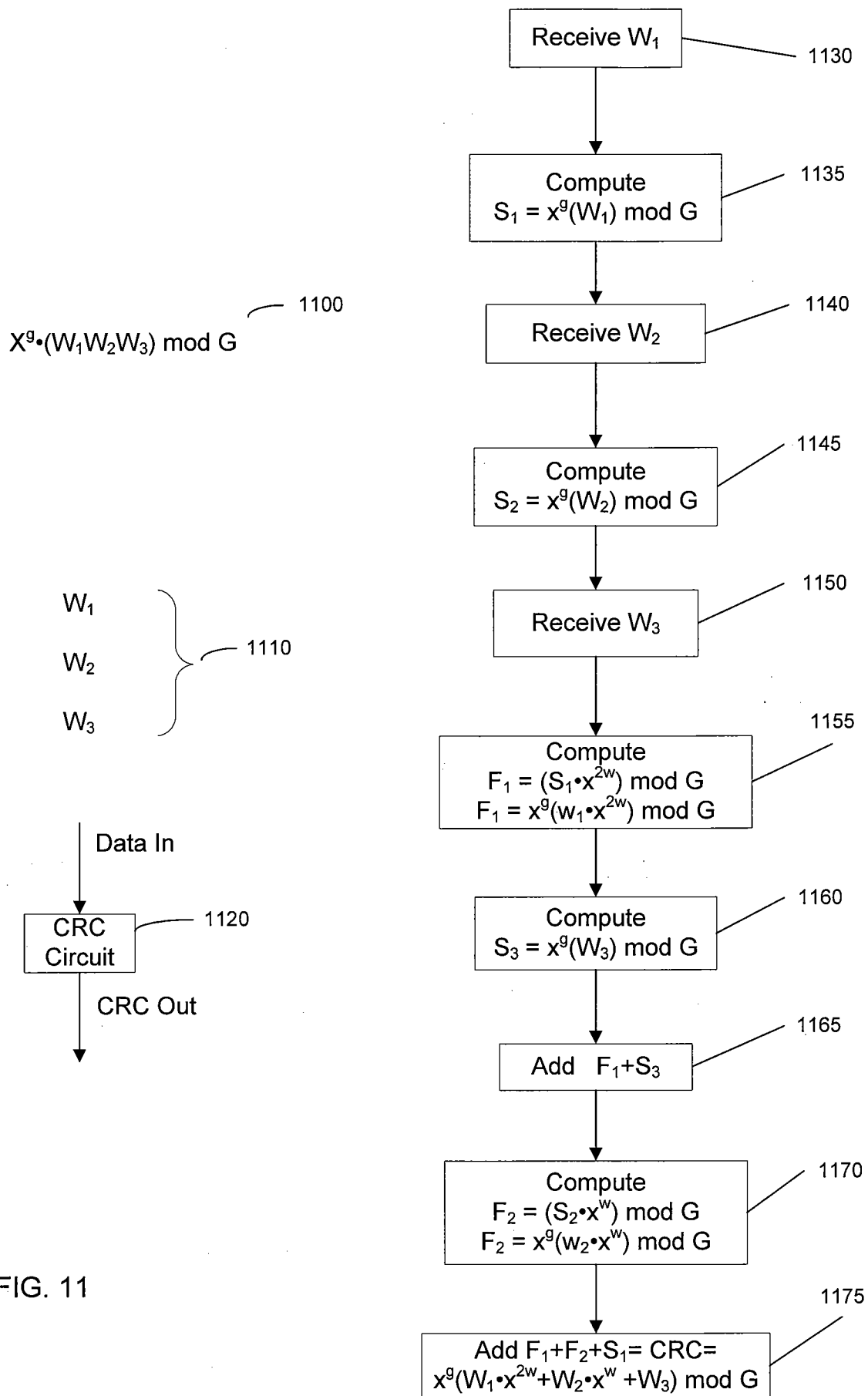


FIG. 11

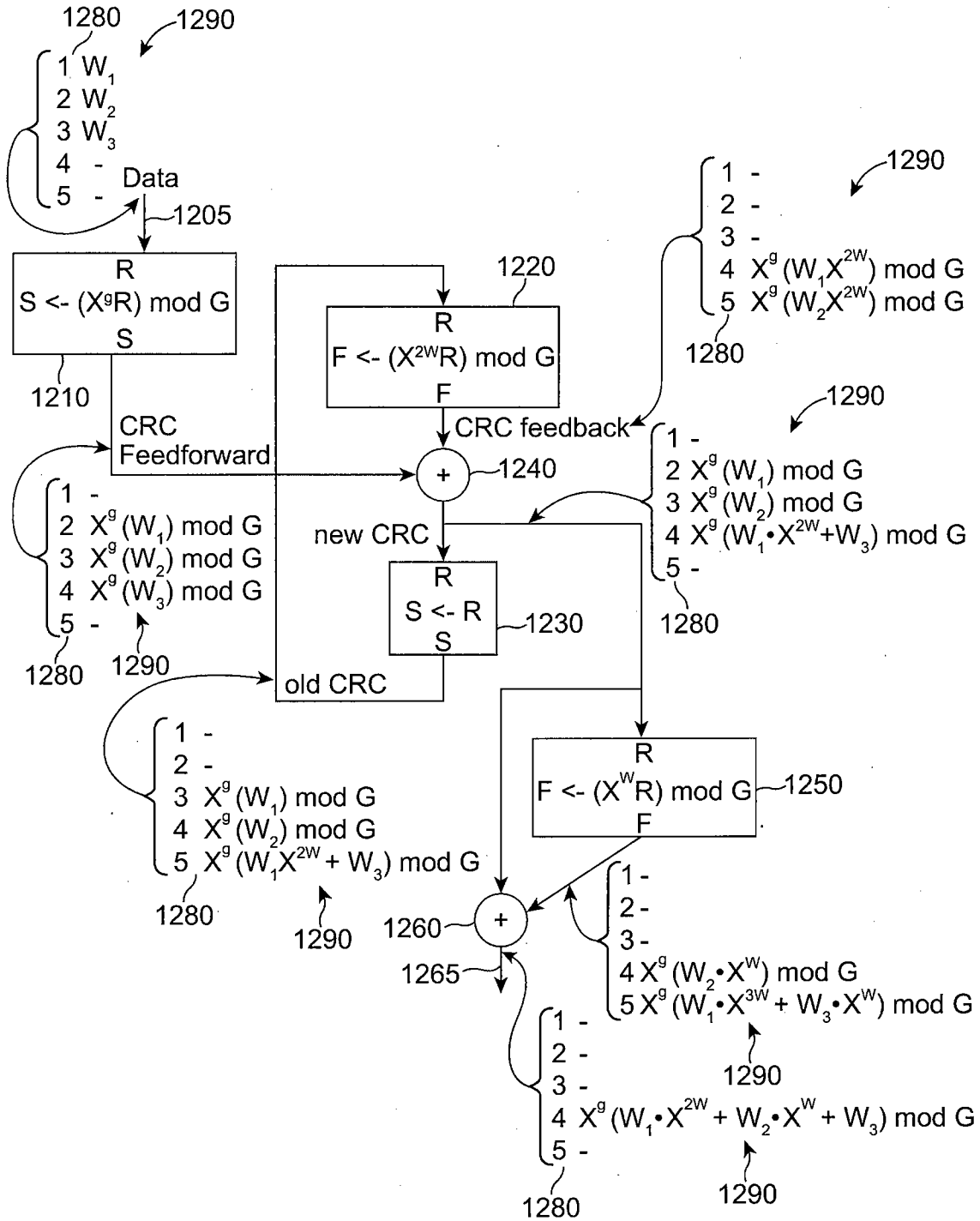


FIG. 12

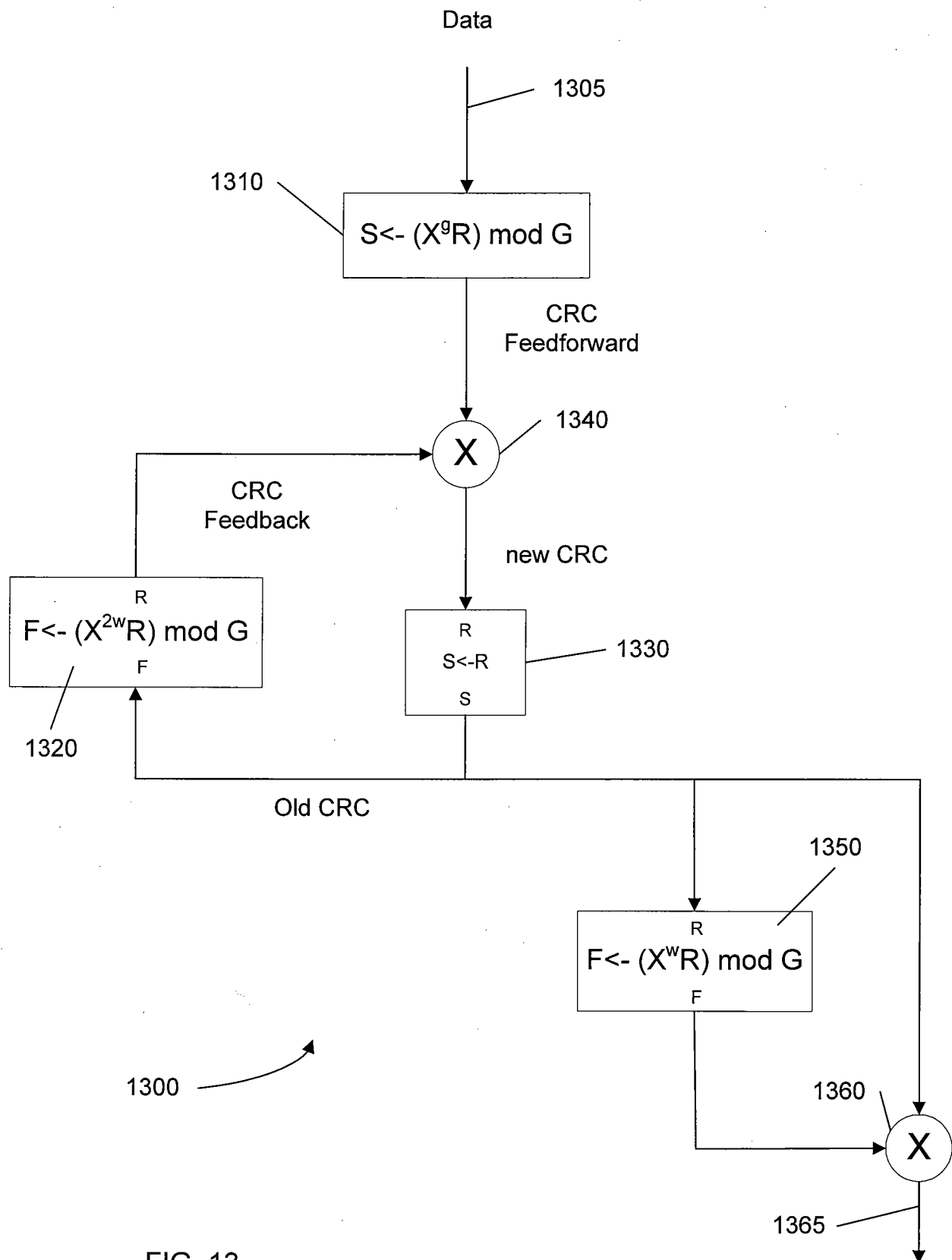


FIG. 13

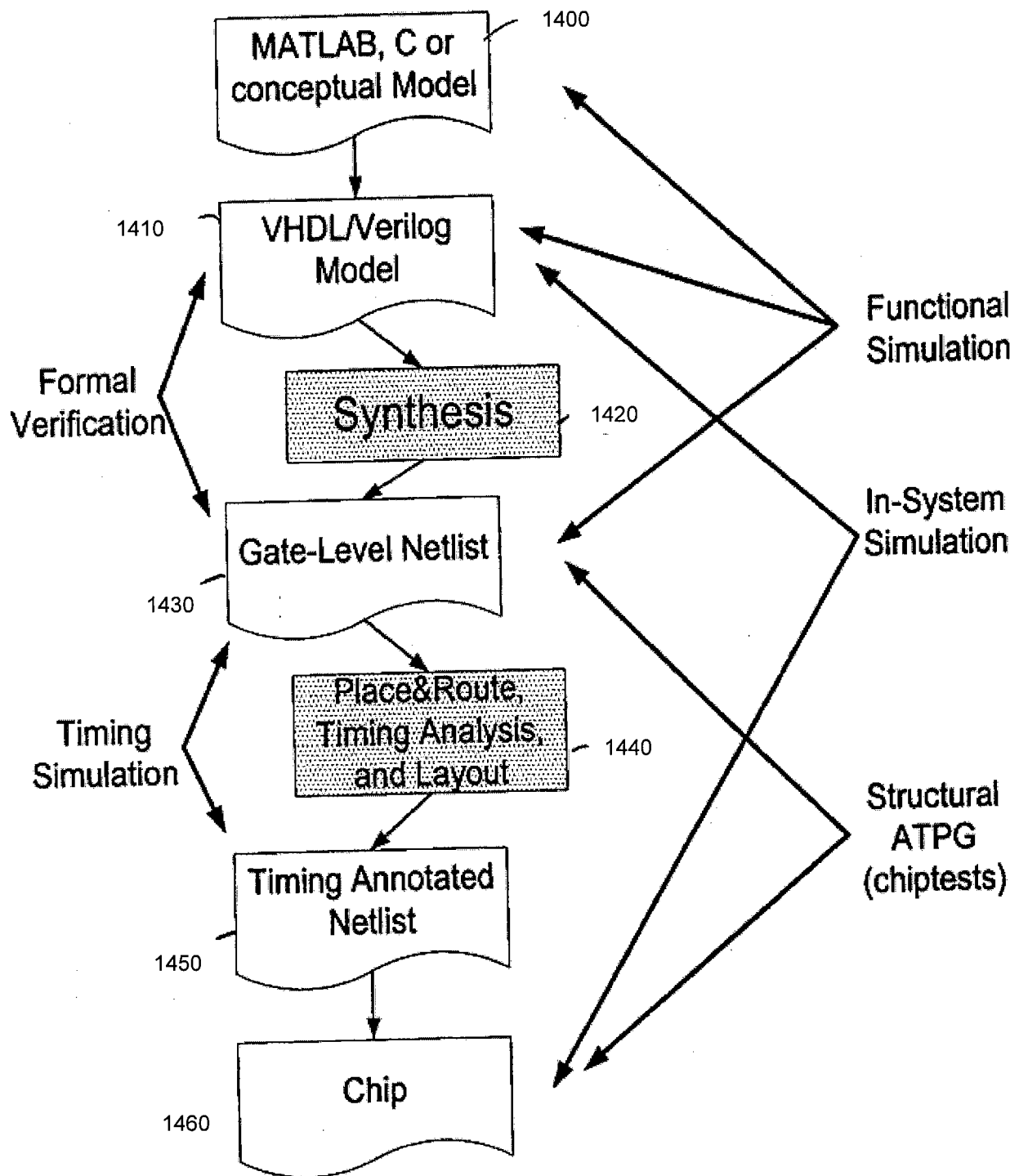


FIG. 14

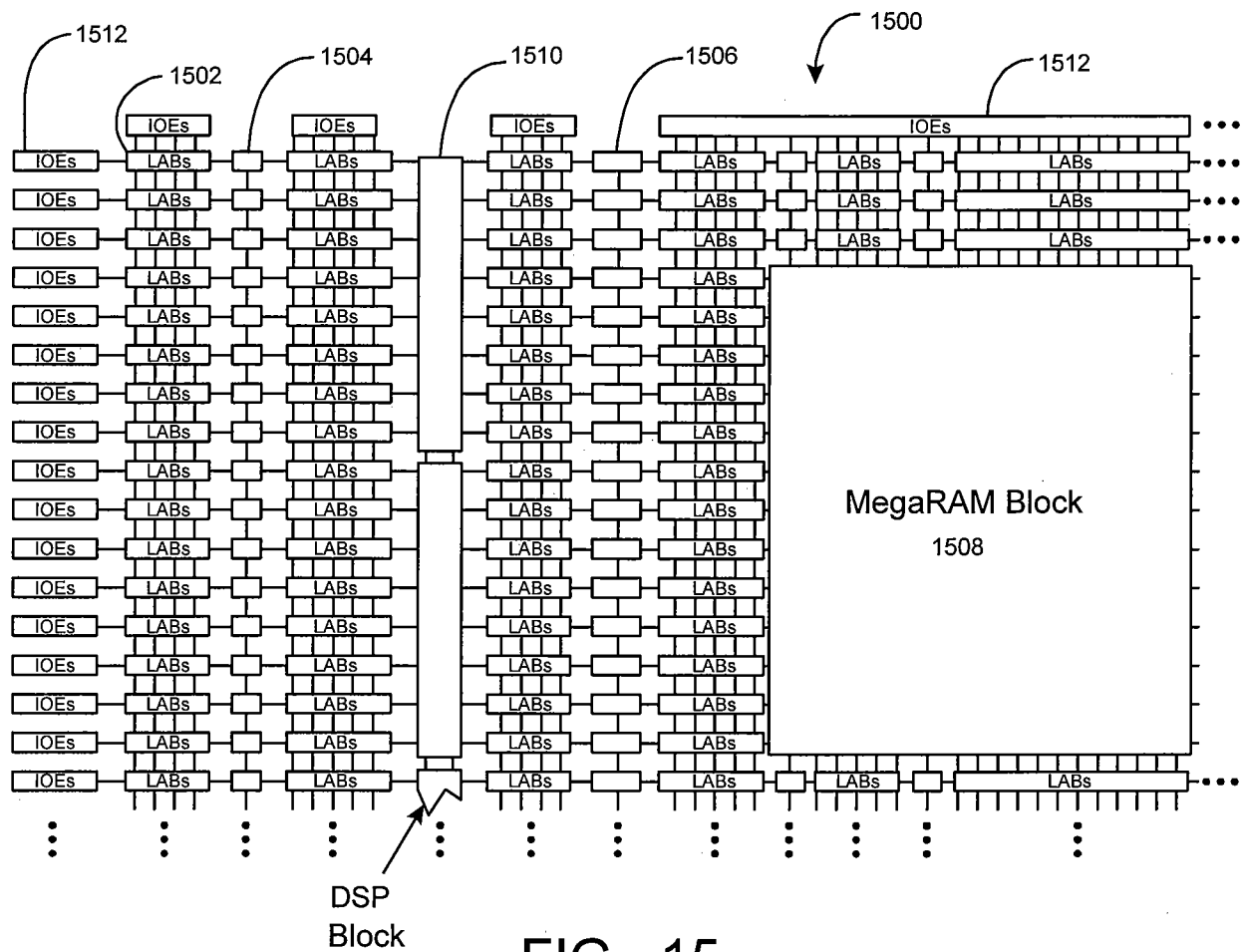


FIG. 15

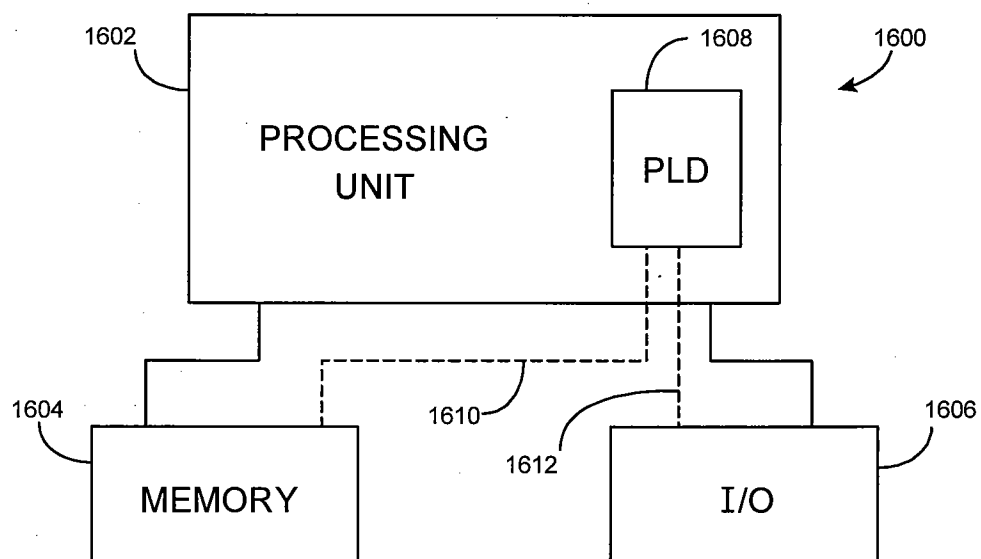


FIG. 16